UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/671,152	09/25/2003	Peter Szor	SYMC1039	4561

34350 7590 03/08/2007

GUNNISON, MCKAY & HODGSON, L.L.P.
1900 GARDEN ROAD, SUITE 220
MONTEREY, CA 93940

EXAMINER	
BAUM, RONALD	
ART UNIT	**PAPER NUMBER**
2136	

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
3 MONTHS	03/08/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

Office Action Summary	Application No.	Applicant(s)	
	10/671,152	SZOR, PETER	
	Examiner	Art Unit	
	Ronald Baum	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *15 March 2006*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-25* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,14,16 and 21-25* is/are rejected.

7)☒ Claim(s) *2-13,15 and 17-20* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *20070228*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This action is in reply to applicant's correspondence of 15 March 2006.

2. Claims 1-25 are pending for examination.

3. Claims 1, 14, 16 and 21-25 are rejected.

Claim Rejections - 35 USC § 101

35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

4. Claims 22-25 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. The phrase "A computer program product comprising" is not necessarily embodied software on computer readable media (subject to inclusion of said subject matter in the specification) corresponding to a method of said embodied software. For the sake of applying art, the examiner assumes that the embodied software of the method is so embodied on computer readable media.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

5. Claims 1, 14, 16 and 21 are rejected under 35 U.S.C. 102(b) as being anticipated by Xenitellis, S., 'Security Vulnerabilities in Event-Driven Systems', ISG, Royal Holloway Univ. of London, 2002, entire document, http://www.isg.rhul.ac.uk/~simos/pub/OLD/SecurityVulnerabilitiesInEvent-drivenSystems.pdf ('Xenitellis').

6. As per claim 1; "A method comprising:

hooking

an exception handler dispatcher [Section 1-5, whereas in an 'event driven model' with the associated system event dispatcher called as part of the operating system kernel, and associated modification or not upon 'condition interception [i.e., after subsequent hooking]' response, encompasses the claimed limitations as broadly interpreted by the examiner.];

stalling execution of

said exception handler dispatcher

upon invocation of

said exception handler dispatcher [Section 1-5, whereas in an 'event driven model' with the associated system event dispatcher called as part of the operating system kernel, and associated modification or not upon 'condition interception' response [i.e., stalling], encompasses the claimed limitations as broadly interpreted by the examiner.]; and

determining whether

an exception handling is valid,

wherein

upon a determination that said exception handling is valid,

said method further comprising

allowing said execution of said exception handler dispatcher

to proceed [Section 1-5, whereas in an 'event driven model' with the associated system event dispatcher called as part of the operating system kernel, and associated modification or not upon 'condition interception' response [i.e., stalling determination as a result of exception processing, and subsequent continuation or not of exception/event], encompasses the claimed limitations as broadly interpreted by the examiner.].".

As per claim 22, this claim is the embodied software claim for the method claim 1 above, and is rejected for the same reasons provided for the claim 1 rejection; "A computer program product comprising:

an exception handling validation application for

hooking

an exception handler dispatcher;

said exception handling validation application further for

stalling execution of

said exception handler dispatcher

upon invocation of

said exception handler dispatcher; and

said exception handling validation application further for

determining whether

an exception handling is valid,

wherein

upon a determination that said exception handling is valid,

said exception handling validation application further for

allowing said execution of said exception handler

dispatcher

to proceed.".

7. Claim 14 ***additionally recites*** the limitation that; "The method of Claim 1 wherein

upon a determination that said exception handling is not valid during said determining, said method further comprising

taking protective action.".

The teachings of Xenitellis are directed towards such limitations (i.e., Section 1-5, whereas in an 'event driven model' with the associated system event dispatcher called as part of the operating system kernel, and associated modification or not upon 'condition interception' response [i.e., stalling determination as a result of exception processing, and subsequent continuation or not ('taking protective action') of exception/event], encompasses the claimed limitations as broadly interpreted by the examiner.).

8. Claim 16 ***additionally recites*** the limitation that; "The method of Claim 14 further comprising

providing a notification that

said protective action has been taken.".

The teachings of Xenitellis are directed towards such limitations (i.e., Section 1-5, whereas in an 'event driven model' with the associated system event dispatcher called as part of the operating system kernel, and associated modification or not upon 'condition interception' response [i.e., stalling determination as a result of exception processing, and subsequent continuation or not ('providing a notification ... taking protective action') of exception/event], encompasses the claimed limitations as broadly interpreted by the examiner.).

9. As per claim 21; "A method comprising:

determining that

exception handling is valid

prior to allowing execution of

an exception handler dispatcher [Section 1-5, whereas in an 'event driven model' with the associated system event dispatcher called as part of the operating system kernel, and associated modification or not upon 'condition interception' response [i.e., determination as a result of exception processing, and subsequent continuation or not (valid/not valid) of exception/event], encompasses the claimed limitations as broadly interpreted by the examiner.].".

Allowable Subject Matter

Claims 2-13, 15, 17-20, 23-25 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims, and subject to the above 35 U.S.C. 101 rejection.

10. Claim 2 ***additionally recites*** the limitation that; "The method of Claim 1 wherein said determining whether an exception handling is valid comprises:

determining whether

exception handler frame addresses are

in order.".

As per claim 23, this claim is the embodied software claim for the method claim 2 above, and is objected to for the same reasons provided for the claim 2 objection; "The computer program product of Claim 22 wherein

said determining whether an exception handling is valid comprises:

determining whether

exception handler frame addresses are

in order.".

11. Claim 3 ***additionally recites*** the limitation that; "The method of Claim 2 wherein said determining whether exception handler frame addresses are in order comprises

determining whether

said exception handler frame addresses are

successively increasing from

a first exception handler frame

located highest on a stack.".

12. Claim 4 ***additionally recites*** the limitation that; "The method of Claim 1 wherein said determining whether an exception handling is valid comprises:

determining whether

an exception handler

is in a data area of memory.".

As per claim 24, this claim is the embodied software claim for the method claim 4 above, and is objected to for the same reasons provided for the claim 4 objection; "The computer program product of Claim 22 wherein

said determining whether an exception handling is valid comprises:

determining whether

an exception handler

is in a data area of memory.".

13. Claim 5 ***additionally recites*** the limitation that; "The method of Claim 4 wherein said determining whether an exception handler is in a data area of memory comprises

determining whether

a handler address in an exception handler frame

points to a page in said data area.".

14. Claim 6 ***additionally recites*** the limitation that; "The method of Claim 1 wherein said determining whether an exception handling is valid comprises:

determining whether

a previous exception handler frame address

is invalid.".

As per claim 25, this claim is the embodied software claim for the method claim 6 above, and is objected to for the same reasons provided for the claim 6 objection; "The computer program product of Claim 22 wherein

said determining whether an exception handling is valid comprises:

determining whether

a previous exception handler frame address

is invalid.".

15. Claim 7 ***additionally recites*** the limitation that; "The method of Claim 6 wherein said determining whether a previous exception handler frame address is invalid comprises

determining whether

said previous exception handler frame address

in an exception handler frame

points to a page that

is invalid.".

16. Claim 8 ***additionally recites*** the limitation that; "The method of Claim 1 wherein exception handler frames form a linked list,

said determining whether an exception handling is valid comprises:

determining whether

exception handler frame addresses of said exception handler frames

are in order.".

17. Claim 9 ***additionally recites*** the limitation that; "The method of Claim 8 wherein said determining whether exception handler frame addresses of said exception handler frames are in order comprises

determining whether

said exception handler frame addresses

are successively increasing from

a first exception handler frame

located highest on a stack,

said linked list comprising

said first exception handler frame.".

18. Claim 10 ***additionally recites*** the limitation that; "The method of Claim 1 wherein

exception handler frames form a linked list,

said determining whether an exception handling is valid comprises:

determining whether

any exception handlers associated with

said exception handler frames

are in a data area of memory.".

19. Claim 11 ***additionally recites*** the limitation that; "The method of Claim I0 wherein said determining whether any exception handlers associated with said exception handler frames are in a data area of memory comprises

determining whether

any handler addresses in said exception handler frames

point to a page in said data area.".

20. Claim 12 ***additionally recites*** the limitation that; "The method of Claim 1 wherein exception handler frames form a linked list,

said determining whether an exception handling is valid comprises:

determining whether

any previous exception handler frame addresses in said exception handler frames

are invalid.".

21. Claim 13 ***additionally recites*** the limitation that; "13. The method of Claim 12 wherein said determining whether any previous exception handler frame addresses in said exception handler frames are invalid comprises

determining whether

said any previous exception handler frame addresses in said exception handler frames

point to a page that is invalid.".

22. Claim 15 ***additionally recites*** the limitation that; "The method of Claim 14 wherein prior to said taking protective action, said method further comprising

determining that

said exception handling

is not a known false positive exception handling.".

23. Claim 17 ***additionally recites*** the limitation that; "The method of Claim 1 wherein said hooking comprises

hooking a function called

KiUserExceptionDispatcher().".

24. Claim 18 ***additionally recites*** the limitation that; "The method of Claim 1 wherein said hooking comprises

modifying said exception handler dispatcher

to redirect flow to

an exception handling validation module.".

25. Claim 19 ***additionally recites*** the limitation that; "The method of Claim 18 wherein said modifying comprises

inserting a jump instruction into

said exception handler dispatcher.".

26. Claim 20 ***additionally recites*** the limitation that; "The method of Claim 1 further comprising

invoking said exception handler dispatcher,

said invoking comprising

raising an exception.".

Conclusion

27. Any inquiry concerning this communication or earlier communications from examiner should be directed to Ronald Baum, whose telephone number is (571) 272-3861, and whose unofficial Fax number is (571) 273-3861 and unofficial email is Ronald.baum@uspto.gov. The examiner can normally be reached Monday through Thursday from 8:00 AM to 5:30 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser Moazzami, can be reached at (571) 272-4195. The Fax number for the organization where this application is assigned is **571-273-8300**.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. For more information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Ronald Baum

Patent Examiner

NASSER MOAZZAMI
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

3/2/07